PATRICK E. PREMO (CSB No. 184915)
ppremo@fenwick.com
SHEEVA J. GHASSEMI-VANNI (CSB No. 246639)
sghassemi@fenwick.com
JOHN-PAUL S. DEOL (CSB No. 284893)
jpdeol@fenwick.com
TIARA R. QUINTANA (CSB No. 315783)
tquintana@fenwick.com
FENWICK & WEST LLP
801 California Street
Mountain View, CA 94041
Telephone: 650.988.8500
Facsimile: 650.938.5200

Attorneys for Plaintiff
GLINT INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

GLINT INC., a Delaware corporation,

Plaintiff,

v.

PERCEPTYX, INC., a California corporation; MITCHELL ANDERSON, an individual; and DOES 1 through 10, inclusive,

Defendants.

CASE NO. 3:18-cv-02886-CRB

DECLARATION OF ANITA HSIUNG CAREY IN SUPPORT OF PLAINTIFF'S EX PARTE APPLICATION FOR A TEMPORARY RESTRAINING ORDER AND MOTION FOR EXPEDITED DISCOVERY

I, Anita Hsiung Carey, declare as follows:

1. I am a Technical Operations Manager and have been employed at Glint Inc. ("Glint") since March 2016.

2. I make this declaration of my own personal knowledge, except to any extent otherwise specified. If called as a witness, I could and would testify competently to the facts set forth herein.

3. I have worked in technical operations since 2012 and I have six and a half years of experience working in the information technology (IT) industry. In my current position as Technical Operations Manager, I handle the IT infrastructure, the backup, the setup, and the security of Glint's proprietary software. I also handle security training for everyone in Glint's IT Department, and set up and maintain all Glint computers.

4. In order to protect its trade secrets and ensure that client data is secure, Glint utilizes various security measures to protect its data on company laptops, in Gmail and G-Suite accounts, and in its Salesforce account.

5. When Glint provides its employees with laptops, either I or one of the members of my team configure the laptop. As part of the configuration, I first encrypt the hard drive to ensure that the data remains private and secure. After the disk is encrypted, I install anti-virus software and employ a firewall to block all ports, which provides protection from remote hackers. In order to secure the encryption keys, all passwords are sent to Glint employees using DataMotion, a security information transportation service that safeguards the security of those passwords so that no one else can intercept them.

6. In or around September 2016, I set up Defendant Mitchell Anderson ("Mr. Anderson")'s Glint laptop and sent it to him at his home in Minneapolis, Minnesota. I made sure the above-mentioned security protocols were in place on Mr. Anderson's computer before I sent it to him.

7. Most of Glint's files, including its survey questions and sales files are stored using Google Drive.

///

8. Glint employees access their Gmail and G-Suite accounts through a two-factor authentication process. First, an employee creates and enters his or her username and password. Second, the employee receives a unique, one-time code on his or her personal mobile phone or through an authenticator application. Using both methods, the employee receives an access code that must be entered into the system for every login from a non-Glint computer.

9. Glint employees using Salesforce access their accounts using Google tokens created in connection with the two-factor authentication process. The Salesforce application authenticates a Glint employee's credentials using the Google tokens, which are encrypted and stored inside the browser. The browser then provides the token each time Salesforce is accessed to verify the employee's identity before allowing access.

10. The above methods of securing Glint's data make it almost impossible for someone without permission to gain access to the Company's data.

11. On or about May 7, 2018, Glint's general counsel, Marc Pappalardo, asked me to review Mr. Anderson's laptop to determine whether he had misappropriated any confidential and proprietary information of Glint.

12. On May 8, 2018 and May 9, 2018, I reviewed Mr. Anderson's downloads folder on his Glint laptop and determined that he had downloaded numerous Glint files from G-Suite to his Glint desktop between April 20, 2018 and April 27, 2018. Based on my experience working for Glint, I recognized these files to be confidential and proprietary Glint sales documents, including files relating to bids and other confidential information regarding deals where Glint is in direct competition with Perceptyx.

13. During my investigation on May 8, 2018 and May 9, 2018, I also reviewed whether Mr. Anderson had attempted to access G-Suite from a non-Glint computer or other electronic device.

14. With assistance from technical support at Google, I was able to determine that five (5) login attempts were made by someone in Los Angeles, California, and Temecula, California to

access G-Suite using Mr. Anderson's Glint login credentials from a non-Glint computer or electronic device. These access attempts occurred on April 30, 2018 and May 1, 2018.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct, and that this declaration was executed this 17th day of May, 2018 in Redwood City, California.

Anita Hsiung Carey